J. Algebra Comb. Discrete Appl.
7(3) • 209–227

Received: 7 September 2019
Accepted: 6 May 2020

Journal of Algebra Combinatorics Discrete Structures and Applications

Self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ and applications*

Research Article

Parinyawat Choosuwan, Somphong Jitman

Abstract: Self-dual codes over finite fields and over some finite rings have been of interest and extensively studied due to their nice algebraic structures and wide applications. Recently, characterization and enumeration of Euclidean self-dual linear codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with $u^3 = 0$ have been established. In this paper, Hermitian self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ are studied for all square prime powers q. Complete characterization and enumeration of such codes are given. Subsequently, algebraic characterization of H-quasi-abelian codes in $\mathbb{F}_q[G]$ is studied, where $H \le G$ are finite abelian groups and $\mathbb{F}_q[H]$ is a principal ideal group algebra. General characterization and enumeration of H-quasi-abelian codes and self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ are given. For the special case where the field characteristic is 3, an explicit formula for the number of self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ is determined for all finite abelian groups A and B such that $3 \nmid |A|$ as well as their construction. Precisely, such codes can be represented in terms of linear codes and self-dual linear codes over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$. Some illustrative examples are provided as well.

2010 MSC: 94B15, 94B05, 94B60

Keywords: Hermitian self-dual linear codes, Quasi-abelian codes, Finite chain rings, Group algebras

1. Introduction

Self-dual linear codes over finite fields form an interesting class of linear codes that have been extensively studied due to their nice algebraic structures and wide applications (see [8], [11], [12], [22] and references therein). Codes over finite rings have been of interest after it was shown that some binary

* *P. Choosuwan was partially supported by the Faculty of Science and Technology, Rajamangala University of Technology Thanyaburi (RMUTT). S. Jitman was supported by the Thailand Research Fund and Silpakorn University under Research Grant RSA6280042.*

Parinyawat Choosuwan; Department of Mathematics and Computer Science, Faculty of Science and Technology, Rajamangala University of Technology Thanyaburi (RMUTT), Pathum Thani 12110, Thailand (email: parinyawat_c@rmutt.ac.th).

Somphong Jitman (Corresponding Author); Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand (email: sjitman@gmail.com).

http://dx.doi.org/10.13069/jacodesmath.784982 ISSN 2148-838X

non-linear codes such as the Kerdock, Preparata and Goethal codes are the Gray images of linear codes over $\mathbb{Z}_4$ in [7]. In general, families of linear codes and self-dual linear codes over finite chain rings are now become of interest. In [16], the mass formula for Euclidean self-dual linear codes over $\mathbb{Z}_{p^3}$ has been studied. Characterization and enumeration of Euclidean self-dual linear codes over the ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with $u^3 = 0$ have been given in [3].

Algebraically structured codes over finite fields such as cyclic codes, abelian codes and quasi-abelian codes are another important family of linear codes that have been extensively studied for both theoretical and practical reasons (see [2], [8], [10], [11], [12] and references therein). In [10], H-quasi-abelian codes and self-dual H-quasi-abelian codes in $\mathbb{F}_q[G]$ have been studied in the case where $\mathbb{F}_q[H]$ is semisimple

To the best of our knowledge, Hermitian self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ and non-semisimple H-quasi-abelian codes in $\mathbb{F}_q[G]$ have not been well studied. The goals of this paper are to investigate the following families of linear codes and their links. 1) Hermitian self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ where q is a square prime power. 2) H-quasi-abelian codes and self-dual H-quasi-abelian codes in group algebras $\mathbb{F}_q[G]$, where $H \leq G$ are finite abelian groups and $\mathbb{F}_q[H]$ is a principal ideal group algebra.

The paper is organized as follows. In Section 2, some results on linear codes and Euclidean self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ are recalled. In Section 3, characterization and enumeration Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ are established for all square prime powers q together with an algorithm to determine all Hermitian self-dual codes and illustrative examples. In Section 4, the study of H-quasi-abelian codes in $\mathbb{F}_q[G]$ is given, where $\mathbb{F}_q[H]$ is a principal ideal group algebra. In the special case where the field characteristic is 3, the characterization and enumeration of $A \times \mathbb{Z}_3$-quasi-abelian codes and self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ are completely determined in terms of linear and self-dual linear codes over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ obtained in Section 3 for all finite abelian groups A and B such that $3 \nmid |A|$. Summary and remarks are given in Section 5.

2. Preliminaries

In this section, basic results on linear codes and Euclidean self-dual linear codes over rings are recalled.

2.1. Linear codes over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$

For a prime power q, denote by $\mathbb{F}_q$ the finite field of order q. Let $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q := \{a_0 + ua_1 + \cdots + u^{e-1}a_{e-1} \mid a_i \in \mathbb{F}_q \text{ for all } 0 \leq i < e\}$ be a ring, where the addition and multiplication are defined as in the usual polynomial ring over $\mathbb{F}_q$ with indeterminate u together with the condition $u^e = 0$. It is easily seen that $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ is isomorphic to $\mathbb{F}_q[u]/\langle u^e \rangle$ as rings. The *Galois extension* of $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ of degree m is defined to be the quotient ring $(\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q)[x]/\langle f(x) \rangle$, where $f(x)$ is an irreducible polynomial of degree m over $\mathbb{F}_q$. It is not difficult to see that the Galois extension of $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ of degree m is isomorphic to $\mathbb{F}_{q^m} + u\mathbb{F}_{q^m} + \cdots + u^{e-1}\mathbb{F}_{q^m}$. The ring $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ is a finite chain ring with maximal ideal $\langle u \rangle$, nilpotency index e and residue field $\mathbb{F}_q$. In addition, if q is a square, the mapping $\bar{\ } : \mathbb{F}_q \to \mathbb{F}_q$ defined by $a \mapsto a^{\sqrt{q}}$ is a field automorphism on $\mathbb{F}_q$ of order 2. Extend $\bar{\ }$ to be a ring automorphism of order 2 on $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$ of the form $\overline{a_0 + ua_1 + \cdots + u^{e-1}a_{e-1}} = \overline{a_0} + u\overline{a_1} + \cdots + u^{e-1}\overline{a_{e-1}}$.

Let n be a positive integer and let R be a finite ring. The *Euclidean inner product* of $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ in R^n is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} := \sum_{i=0}^{n-1} u_i v_i.$$

In the case where q is a square and $R \in \{\mathbb{F}_q, \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q\}$, the *Hermitian inner product* of $\boldsymbol{u}$

and $\boldsymbol{v}$ in R^n is defined to be

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} := \sum_{i=0}^{n-1} u_i \overline{v_i}.$$

A *linear code* $\mathcal{C}$ of length n over the ring R is defined to be an R-submodule of the R-module R^n. A linear code over R is said to be *free* if it is a free R-module. Denote by $\mathrm{wt}(\boldsymbol{v})$ the Hamming weight of an element $\boldsymbol{v} \in R^n$. Precisely, $\mathrm{wt}(\boldsymbol{v})$ is the number of non-zero components in $\boldsymbol{v}$. For a linear code $\mathcal{C}$ over R, let $\mathrm{wt}(\mathcal{C}) = \min\{\mathrm{wt}(\boldsymbol{c}) \mid \boldsymbol{c} \in \mathcal{C}\}$ be the minimum Hamming weight of $\mathcal{C}$. If $R = \mathbb{F}_q$, a linear code $\mathcal{C}$ of length n and dimension k over R with $\mathrm{wt}(\mathcal{C}) = d$ is referred as an $[n, k, d]_q$ code. The parameters of a linear code $\mathcal{C}$ of length n over R satisfies the Singleton bond [14], i.e., $\mathrm{wt}(\mathcal{C}) \leq n - \log_{|R|}(|\mathcal{C}|) + 1$. A linear code $\mathcal{C}$ is called a *Maximum Distance Separable (MDS) code* if the equality in the Singleton bound holds. A matrix G over R is called a *generator matrix* for $\mathcal{C}$ if the rows of G generate all the elements of $\mathcal{C}$ and none of the rows can be written as a linear combination of the others. Linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over R are said to be *equivalent* if there exists a monomial matrix P such that $\mathcal{C}_2 = \mathcal{C}_1 P := \{\boldsymbol{c}P \mid \boldsymbol{c} \in \mathcal{C}_1\}$. Denote by $\mathcal{C}^{\perp_{\mathrm{E}}} = \{\boldsymbol{v} \in R^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} = 0\}$ and $\mathcal{C}^{\perp_{\mathrm{H}}} = \{\boldsymbol{v} \in R^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = 0\}$ the *Euclidean* and *Hermitian duals* of $\mathcal{C}$, respectively. A linear code $\mathcal{C}$ is said to be *Euclidean* (resp., *Hermitian*) *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^{\perp_{\mathrm{E}}}$ (resp., $\mathcal{C} \subseteq \mathcal{C}^{\perp_{\mathrm{H}}}$). It is called *Euclidean* (resp., *Hermitian*) *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp_{\mathrm{E}}}$ (resp., $\mathcal{C} = \mathcal{C}^{\perp_{\mathrm{H}}}$).

In Section 3 and the remaining parts of this section, we focus on linear and self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. In [19], it has been shown that every linear code of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ is permutation equivalent to a code $\mathcal{C}$ with generator matrix

$$G = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & uI_l & uB_3 & uB_4 \\ 0 & 0 & u^2 I_m & u^2 C_4 \end{bmatrix} = \begin{bmatrix} A' \\ uB' \\ u^2 C \end{bmatrix}, \tag{1}$$

where I_r is the identity matrix of order r, $A_3 = A_{30} + uA_{31}, B_4 = B_{40} + uB_{41}, A_4 = A_{40} + uA_{41} + u^2 A_{42}$, and A_2, B_3, C_4, A_{ij} and B_{ij} are matrices of appropriate sizes over $\mathbb{F}_q$. In this case, the code $\mathcal{C}$ is said to be of type $\{k, l, m\}$ and it contains $q^{3k+2l+m}$ codewords.

For each linear code $\mathcal{C}$ of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ and $i \in \{0, 1, 2\}$, the ith *torsion code* of $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_q$ defined to be

$$\mathrm{Tor}_i(\mathcal{C}) = \left\{ \boldsymbol{v} (\mathrm{mod} u) \mid \boldsymbol{v} \in \left(\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q\right)^n \text{ and } u^i \boldsymbol{v} \in \mathcal{C} \right\}.$$

The code $\mathrm{Tor}_0(\mathcal{C})$ is sometime called the *residue code* of $\mathcal{C}$ and denoted it by $\mathrm{Res}(\mathcal{C})$. From the definitions, it is obvious that $\mathrm{Res}(\mathcal{C}) = \mathrm{Tor}_0(\mathcal{C}) \subseteq \mathrm{Tor}_1(\mathcal{C}) \subseteq \mathrm{Tor}_2(\mathcal{C})$.

For a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix G given in (1), the residue code $\mathrm{Res}(\mathcal{C})$ has dimension k and generator matrix

$$G = \begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \end{bmatrix}, \tag{2}$$

the first torsion code $\mathrm{Tor}_1(\mathcal{C})$ has dimension $k + l$ and generator matrix

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \\ 0 & I_l & B_3 & B_{40} \end{bmatrix}, \tag{3}$$

and the second torsion code $\mathrm{Tor}_2(\mathcal{C})$ has dimension $k + l + m$ and generator matrix

$$\begin{bmatrix} A \\ B \\ C \end{bmatrix} = \begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \\ 0 & I_l & B_3 & B_{40} \\ 0 & 0 & I_m & C_4 \end{bmatrix}. \tag{4}$$

For $0 \leq k \leq n$, the *Gaussian coefficient* is defined to be

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.$$

Let $N_e(q,n)$ denote the number of distinct linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$. The number $N_e(q,n)$ has been studied and summarized in [4]. For $e = 3$, we have the following result.

Proposition 2.1 ([4, Lemma 2.2])**.** *Let q be a prime power and let n be a positive integer. Then*

$$N_3(q,n) = 1 + \sum_{t=1}^{3} \sum_{n \geq h_1 \geq h_2 \geq \cdots \geq h_t > h_{t+1} = 0} \prod_{j=1}^{t} \begin{bmatrix} n - h_{j+1} \\ h_j - h_{j+1} \end{bmatrix}_q q^{h_{j+1}(n-h_j)}.$$

2.2. Euclidean self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$

Let $\mathcal{C}$ be a linear code of length n and type $\{k,l,m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ and let $h = n-(k+l+m)$. In [3], it has been shown that the Euclidean dual $\mathcal{C}^{\perp_{\rm E}}$ of $\mathcal{C}$ is of type $\{h,m,l\}$ and it contains $q^{3h+2m+l}$ codewords. Therefore, $k = h$ and $l = m$ whenever $\mathcal{C}$ is Euclidean self-dual. Consequently, every Euclidean self-dual code of type $\{k,l,m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ has even length $n = 2(k+l)$.

Characterization of Euclidean self-dual linear codes of even length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ has been established in [3].

Proposition 2.2 ([3, Proposition 1])**.** *Let q be a prime power and let $\mathcal{C}$ be a linear code of length n and type $\{k,l,m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix G in the form of (1). Then $\mathcal{C}$ is Euclidean self-dual if and only if $k = h, l = m$ and the following conditions hold:*

$$A'A'^T \equiv 0 \pmod{u^3}, \tag{5}$$

$$A'B'^T \equiv 0 \pmod{u^2}, \tag{6}$$

$$B'B'^T \equiv 0 \pmod{u}, \tag{7}$$

$$A'C^T \equiv 0 \pmod{u}. \tag{8}$$

For a positive integer n and a prime power q, let $\sigma_{\rm E}(q,n)$ denote the number of Euclidean self-dual linear codes of length n over $\mathbb{F}_q$. Further, if q is a square prime power, let $\sigma_{\rm H}(q,n)$ denote the number of Hermitian self-dual linear codes of length n over $\mathbb{F}_q$. The following results in [21] and [22] are useful in the enumeration of self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$.

Lemma 2.3 ([21] and [22])**.** *Let q be a prime power and let n be a positive integer. Then*

$$\sigma_{\rm E}(q,l) = \begin{cases} \prod_{i=1}^{\frac{n}{2}-1} (q^i + 1) & \text{if } q \text{ and } n \text{ are even,} \\ 2\prod_{i=1}^{\frac{n}{2}-1} (q^i + 1) & \text{if } q \equiv 1 \,(\mathrm{mod}\, 4) \text{ and } 2 \mid n, \\ 2\prod_{i=1}^{\frac{n}{2}-1} (q^i + 1) & \text{if } q \equiv 3 \,(\mathrm{mod}\, 4) \text{ and } 4 \mid n, \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

If q is square, then

$$\sigma_{\rm H}(q,n) = \begin{cases} \prod_{i=0}^{\frac{n}{2}-1} (q^{i+\frac{1}{2}} + 1) & \text{if } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

The empty product is regarded as 1.

Let $NE_e(q,n)$ denote the number of distinct Euclidean self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$. The value of $NE_3(q,n)$ has been completely determined in [3].

Theorem 2.4 ([3, Theorem 1])**.** *Let q be a prime power and let n be a positive integer. Then*

$$NE_3(q,n) = \begin{cases} \sigma_{\mathrm{E}}(q,n) \displaystyle\sum_{k=0}^{n/2} \begin{bmatrix} \frac{n}{2} \\ k \end{bmatrix}_q q^{kn/2} & \text{if } q \text{ is even and } n \text{ is even,} \\ \sigma_{\mathrm{E}}(q,n) \displaystyle\sum_{k=0}^{n/2} \begin{bmatrix} \frac{n}{2} \\ k \end{bmatrix}_q q^{k(n/2-1)} & \text{if } q \text{ is odd and } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

3. Hermitian self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$

In this section, we focus on characterization and enumeration of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$.

Throughout this section, we assume that q is a square prime power. For each positive integer n, let $NH_e(q,n)$ denote the number of distinct Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{e-1}\mathbb{F}_q$. By extending techniques introduced in [3], the characterization and the number $NH_3(q,n)$ of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ are established.

Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ of type $\{k,l,m\}$ and let $h = n-(k+l+m)$. Using argument similar to those in Section 2 of [3], it can be deduced that the Hermitian dual $\mathcal{C}^{\perp_{\mathrm{H}}}$ of $\mathcal{C}$ is of type $\{h,m,l\}$ and it contains $q^{3h+2m+l}$ codewords. It follows that $k=h$ and $l=m$ if $\mathcal{C}$ is Hermitian self-dual. Hence, every Hermitian self-dual code of type $\{k,l,m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ has even length $n = 2(k+l)$.

For a matrix $A = [a_{ij}]_{s\times t}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, let $\overline{A} := [\overline{a_{ij}}]_{s\times t}$ and $A^\dagger := \overline{A}^T$. Characterization of Hermitian self-dual linear codes of even length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ is given in the following proposition.

Proposition 3.1. *Let q be a square prime power and let $\mathcal{C}$ be a linear code of even length n and type $\{k,l,m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix G in the form of* (1)*. Then $\mathcal{C}$ is Hermitian self-dual if and only if $k=h$, $l=m$ and the following hold:*

$$A'A'^\dagger \equiv 0 \pmod{u^3}, \tag{11}$$
$$A'B'^\dagger \equiv 0 \pmod{u^2}, \tag{12}$$
$$B'B'^\dagger \equiv 0 \pmod{u}, \tag{13}$$
$$A'C^\dagger \equiv 0 \pmod{u}. \tag{14}$$

Proof. Assume that $\mathcal{C}$ is Hermitian self-dual. By the above discussion, we have $k=h$, $l=m$ and

$$\begin{bmatrix} A' \\ uB' \\ u^2C \end{bmatrix} \begin{bmatrix} A' \\ uB' \\ u^2C \end{bmatrix}^\dagger \equiv [0] \pmod{u^3}$$

which are equivalent to the conditions (11)–(14).

Conversely, assume that $\mathcal{C}$ is a linear code such that $k = h, l = m$ and the conditions (11)–(14) hold. From (11)–(14), it is not difficult to see that $\mathcal{C}$ is Hermitian self-orthogonal. Equivalently, $\mathcal{C} \subseteq \mathcal{C}^{\perp_{\rm H}}$. Since $k = h$ and $l = m$, we have $|\mathcal{C}| = |\mathcal{C}^{\perp_{\rm H}}|$ which implies that $\mathcal{C} = \mathcal{C}^{\perp_{\rm H}}$. Therefore, $\mathcal{C}$ is Hermitian self-dual as desired. $\square$

Corollary 3.2. *Let $\mathcal{C}$ be a Hermitian self-dual linear code of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. Then the following statements holds.*

1) $\mathrm{Tor}_1(\mathcal{C})$ *is a Hermitian self-dual code of length n over $\mathbb{F}_q$.*

2) $\mathrm{Tor}_2(\mathcal{C}) = \mathrm{Res}(\mathcal{C})^{\perp_{\rm H}}$.

Proof. Assume that $\mathcal{C}$ is of type $\{k, l, m\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. Then From (11)–(13), it follows that $\mathrm{Tor}_1(\mathcal{C})$ is Hermitian self-orthogonal. Since $\dim(\mathrm{Tor}_1(\mathcal{C})) = k + l = \frac{n}{2} = \dim((\mathrm{Tor}_1(\mathcal{C}))^{\perp_{\rm H}})$, $\mathrm{Tor}_1(\mathcal{C})$ is Hermitian self-dual. From (11)–(14), we have $\mathrm{Tor}_2(\mathcal{C}) \subseteq \mathrm{Res}(\mathcal{C})^{\perp_{\rm H}}$. Since $\dim(\mathrm{Tor}_2(\mathcal{C})) = k + 2l = n - k = \dim((\mathrm{Res}(\mathcal{C}))^{\perp_{\rm H}})$, we have $\mathrm{Tor}_2(\mathcal{C}) = \mathrm{Res}(\mathcal{C})^{\perp_{\rm H}}$. $\square$

Since $\mathrm{Res}(\mathcal{C}) = \mathrm{Tor}_0(\mathcal{C}) \subseteq \mathrm{Tor}_1(\mathcal{C}) \subseteq \mathrm{Tor}_2(\mathcal{C})$, it can be concluded further that $\mathrm{Res}(\mathcal{C})$ is Hermitian self-orthogonal for all Hermitian self-dual linear codes $\mathcal{C}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$.

From Corollary 3.2, a Hermitian self-dual code $\mathcal{C}$ of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ can be induced by Hermitian self-dual linear codes of length n over $\mathbb{F}_q$. For a given Hermitian self-dual code $\mathcal{C}_1$ of length n over $\mathbb{F}_q$, we first aim to determine the number of Hermitian self-dual linear codes $\mathcal{C}$ of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ such that $\mathrm{Tor}_1(\mathcal{C}) = \mathcal{C}_1$.

Proposition 3.3. *Let q be a square prime power and let n be an even positive integer. Let $\mathcal{C}_1$ be a Hermitian self-dual linear code of length n over $\mathbb{F}_q$. Then, for each $0 \leq k \leq \frac{n}{2}$, there are $q^{\frac{kn}{2}}$ Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ corresponding to each subspace of $\mathcal{C}_1$ of dimension k.*

Proof. Let $\mathcal{C}_1$ be a Hermitian self-dual linear code of length n over $\mathbb{F}_q$ with dimension $\frac{n}{2} = k + l$ and generator matrix

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \\ 0 & I_l & B_3 & B_{40} \end{bmatrix}, \tag{15}$$

where the columns are grouped into blocks of sizes k, l, l and k.

Since $\mathcal{C}_1$ is Hermitian self-dual, we have

$$I_k + A_2A_2^\dagger + A_{30}A_{30}^\dagger + A_{40}A_{40}^\dagger = 0, \tag{16}$$
$$A_2 + A_{30}B_3^\dagger + A_{40}B_{40}^\dagger = 0, \tag{17}$$
$$I_l + B_3B_3^\dagger + B_{40}B_{40}^\dagger = 0. \tag{18}$$

Let $H = \begin{bmatrix} A_{30} & A_{40} \\ B_3 & B_{40} \end{bmatrix}$. From (16)–(18), it can be deduced that

$$\begin{aligned} H(-H^\dagger) &= -HH^\dagger \\ &= -H\overline{H}^T \\ &= \begin{bmatrix} -\overline{A_{30}}A_{30}^T - \overline{A_{40}}A_{40}^T & -\overline{A_{30}}B_3^T - \overline{A_{40}}B_{40}^T \\ \left(-\overline{A_{30}}B_3^T - \overline{A_{40}}B_{40}^T\right)^T & -\overline{B_3}B_3^T - \overline{B_{40}}B_{40}^T \end{bmatrix} \\ &= \begin{bmatrix} I_k + \overline{A_2}A_2^T & \overline{A_2} \\ A_2^T & I_l \end{bmatrix}. \end{aligned}$$

Let $J = \begin{bmatrix} I_k & -\overline{A_2} \\ -A_2^T & I_l + A_2^T\overline{A_2} \end{bmatrix}$. Then $H(-H^\dagger)J = \begin{bmatrix} I_k & 0 \\ 0 & I_l \end{bmatrix}$ which implies that H is invertible.

Let $\mathcal{C}_0$ be a k-dimensional $\mathbb{F}_q$-subspace of $\mathcal{C}_1$ with generator matrix A. Since $\mathcal{C}_1$ is Hermitian self-dual, it follows that $\mathcal{C}_0$ is Hermitian self-orthogonal. Up to permutation of the last $(k+l)$ columns (if necessary), its follows that $\mathcal{C}_0^{\perp_{\rm H}}$ has a generator matrix of the form

$$\begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \\ 0 & I_l & B_3 & B_{40} \\ 0 & 0 & I_l & C_4 \end{bmatrix}. \tag{19}$$

Then $A_{30} = -A_{40}C_4^\dagger$ which implies that $H = \begin{bmatrix} -\overline{A_{40}}C_4^T & \overline{A_{40}} \\ \overline{B_3} & \overline{B_{40}} \end{bmatrix}$. Since H is invertible, it follows that A_{40} is invertible.

Next, we determined the matrices over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ satisfying conditions (11)–(14) which are equivalent to

$$I_k + A_2A_2^\dagger + A_3A_3^\dagger + A_4A_4^\dagger \equiv 0 \pmod{u^3} \tag{20}$$
$$A_2 + A_3B_3^\dagger + A_4B_4^\dagger \equiv 0 \pmod{u^2} \tag{21}$$
$$I_l + B_3B_3^\dagger + B_4B_4^\dagger \equiv 0 \pmod{u} \tag{22}$$
$$A_3 + A_4C_4^\dagger \equiv 0 \pmod{u}. \tag{23}$$

The matrices A_2, B_3 and C_4 are considered modulo u, i.e. all the entries in A_2, B_3 and C_4 are in $\mathbb{F}_q$. The matrices A_3 and B_4 are considered modulo u^2 while A_4 is considered modulo u^3. From these fact, let $A_3 = A_{30} + uA_{31}, B_4 = B_{40} + uB_{41}$ and $A_4 = A_{40} + uA_{41} + u^2A_{42}$, where A_{31}, B_{41}, A_{41} and A_{42} are matrices of appropriate sizes over $\mathbb{F}_q$. Therefore, we can write (20) as

$$\left(I_k + A_2A_2^\dagger + A_{30}A_{30}^\dagger + A_{40}A_{40}^\dagger\right) + u\left(\widetilde{A_{30}A_{31}^\dagger} + \widetilde{A_{40}A_{41}^\dagger}\right)$$
$$+u^2\left(A_{31}A_{31}^\dagger + A_{41}A_{41}^\dagger + \widetilde{A_{40}A_{42}^\dagger}\right) \equiv 0 \pmod{u^3},$$

where $\widetilde{X} := X + X^\dagger$. We can also rewrite (21) as

$$\left(A_2 + A_{30}B_3^\dagger + A_{40}B_{40}^\dagger\right) + u\left(A_{31}B_3^\dagger + A_{40}B_{41}^\dagger + A_{41}B_{40}^\dagger\right) \equiv 0 \pmod{u^2}$$

By substituting (18) into (21), we obtain that

$$B_{41}^\dagger = -A_{40}^{-1}\left(A_{31}B_3^\dagger + A_{41}B_{40}^\dagger\right),$$

From (23), C_4 is uniquely determined as

$$C_4 = \left(-A_{40}^{-1}A_{30}\right)^\dagger.$$

It is sufficient to focus on (20) because (18) is the same as (22). From (16), we have to determined the matrices satisfying the following:

$$\widetilde{A_{30}A_{31}^\dagger} + \widetilde{A_{40}A_{41}^\dagger} = 0, \tag{24}$$
$$A_{31}A_{31}^\dagger + A_{41}A_{41}^\dagger + \widetilde{A_{40}A_{42}^\dagger} = 0. \tag{25}$$

Hence, the code $\mathcal{C}$ with generator matrix of the form (1) is a Hermitian self-dual linear code if and only if conditions (24) and (25) are satisfied.

Therefore, the number of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ whose the 1st torsion is $\mathcal{C}_1$ is equal to the number of solutions of the system of matrix equations (24) and (25).

We take an arbitrary matrix $A_{31} \in M_{k\times l}(\mathbb{F}_q)$ and put $[g_{ij}] = \widetilde{A_{30}A_{31}^{\dagger}}$ and $[x_{ij}] = A_{40}A_{41}^{\dagger}$. Then condition (24) is equivalent to

$$g_{ij} + x_{ij} + \overline{x_{ji}} = 0.$$

Then $-g_{ii} = x_{ii} + \overline{x_{ii}} = \mathrm{Tr}(x_{ii}) \in \mathbb{F}_{\sqrt{q}}$ for each $1 \le i \le k$, where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_{\sqrt{q}}$ is the *trace map* defined by $\alpha \mapsto \overline{\alpha} + \alpha$ for all $\alpha \in \mathbb{F}_q$. Note that $|\,\mathrm{Tr}^{-1}(a)| = \sqrt{q}$ for all $a \in \mathbb{F}_{\sqrt{q}}$. Then we have $x_{ii} \in \mathrm{Tr}^{-1}(-g_{ii})$ for all $1 \le i \le k$, $x_{ji} \in \mathbb{F}_q$ and $x_{ij} = -g_{ij} - \overline{x_{ji}}$ for each $1 \le i < j \le k$. Therefore,

$$A_{41} = (A_{40}^{-1}[x_{ij}])^{\dagger}.$$

Thus we have q^{kl} possible choices for A_{31} and $q^{\frac{k(k-1)}{2}+\frac{k}{2}} = q^{\frac{k^2}{2}}$ for A_{41}.

For fixed matrices A_{31} and A_{41}, let $[h_{ij}] = A_{31}A_{31}^{\dagger} + A_{41}A_{41}^{\dagger}$ and $[y_{ij}] = A_{40}A_{42}^{\dagger}$. Then (25) is equivalent to

$$h_{ij} + y_{ij} + \overline{y_{ji}} = 0.$$

Using a similar argument as above, we have $q^{\frac{k^2}{2}}$ possible choices for

$$A_{42} = (A_{40}^{-1}[y_{ij}])^{\dagger}.$$

Therefore, we have

$$q^{kl} \times q^{\frac{k^2}{2}} \times q^{\frac{k^2}{2}} = q^{k^2+kl} = q^{k(k+l)} = q^{\frac{kn}{2}}$$

possible choices for the matrices A_{31}, A_{41} and A_{42} over $\mathbb{F}_q$. Therefore, the desired result follows immediately. $\square$

The number of distinct Hermitian self-dual linear codes of even length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ can be summarized in the following theorem.

Theorem 3.4. *Let q be a square prime power and let n be a positive integer. Then the number of distinct Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ is*

$$NH_3(q,n) = \begin{cases} \sigma_{\mathrm{H}}(q,n) \displaystyle\sum_{k=0}^{n/2} \begin{bmatrix} \frac{n}{2} \\ k \end{bmatrix}_q q^{kn/2} & \text{if } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

From the proof of Theorem 3.3, we obtain not only the number of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ but also a construction of such Hermitian self-dual linear codes. The construction of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ induced by a Hermitian self-dual linear code of length n over $\mathbb{F}_q$ in the proof of Theorem 3.3 is summarized in Algorithm 1.

Based on Algorithm 1, an illustrative example of a Hermitian self-dual linear code of length 6 over $\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9$ constructed from a Hermitian self-dual linear code of length 6 over $\mathbb{F}_9$ is given as follows.

Example 3.5. *Let $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$ be the finite field of order 9, where α is a root of $x^2 + x + 2$ over $\mathbb{F}_3$. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be linear codes of length 6 over $\mathbb{F}_9$ with generator matrices*

$$\left[\begin{array}{cc|c|c|cc} 1 & 0 & 1 & \alpha^2 & \alpha^5 & \alpha^2 \\ 0 & 1 & 0 & \alpha & 1 & \alpha \end{array}\right] \text{ and } \left[\begin{array}{cc|c|c|cc} 1 & 0 & 1 & \alpha^2 & \alpha^5 & \alpha^2 \\ 0 & 1 & 0 & \alpha & 1 & \alpha \\ \hline 0 & 0 & 1 & \alpha^5 & \alpha & 1 \end{array}\right],$$

Algorithm 1. **Construction of Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$**

For a given Hermitian self-dual linear code $\mathcal{C}_1$ of length n over $\mathbb{F}_q$ and its linear subcode $\mathcal{C}_0$ of dimension $0 \le k \le \frac{n}{2}$, do the following steps.

1. Define $l = \frac{n}{2} - k$.
2. Construct a generator matrix $A = \begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \end{bmatrix}$ for $\mathcal{C}_0$, where the columns are grouped into blocks of sizes k, l, l and k.
3. Extend A to be a generator matrix $\begin{bmatrix} I_k & A_2 & A_{30} & A_{40} \\ 0 & I_l & B_3 & B_{40} \end{bmatrix}$ for $\mathcal{C}_1$.
4. Set $C_4 = -\left(A_{40}^{-1} A_{30}\right)^\dagger$.
5. Set A_{31} to be a $k \times l$ matrix over $\mathbb{F}_q$.
6. Define $[g_{ij}] = \widetilde{A_{30} A_{31}^\dagger}$ and set $[x_{ij}]$ to be a $k \times k$ matrix over $\mathbb{F}_q$ such that the strictly lower triangular elements are arbitrary in $\mathbb{F}_q$, $x_{ii} \in \mathrm{Tr}^{-1}(-g_{ii})$, and $x_{ij} = -g_{ij} - \overline{x_{ji}}$ for all $i < j$. (If $k = \frac{n}{2}$, set $[g_{ij}]$ to be the $k \times k$ zero matrix over $\mathbb{F}_q$.)
7. Set $A_{41} = (A_{40}^{-1}[x_{ij}])^\dagger$.
8. Set $B_{41} = -\left(A_{40}^{-1}\left(A_{31}B_3^\dagger + A_{41}B_{40}^\dagger\right)\right)^\dagger$.
9. Define $[h_{ij}] = A_{31}A_{31}^\dagger + A_{41}A_{41}^\dagger$ and set $[y_{ij}]$ to be a $k \times k$ matrix over $\mathbb{F}_q$ such that the strictly lower triangular elements are arbitrary in $\mathbb{F}_q$, $y_{ii} \in \mathrm{Tr}^{-1}(-h_{ii})$, and $y_{ij} = -g_{ij} - \overline{x_{ji}}$ for all $i < j$. (If $k = \frac{n}{2}$, set $[h_{ij}] = A_{41}A_{41}^\dagger$.)
10. Set $A_{42} = (A_{40}^{-1}[y_{ij}])^\dagger$.
11. Define $\mathcal{C}$ to be a linear code of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix
$$\begin{bmatrix} I_k & A_2 & A_{30} + uA_{31} & A_{40} + uA_{41} + u^2A_{42} \\ 0 & uI_l & uB_3 & uB_{40} + u^2B_{41} \\ 0 & 0 & u^2I_l & u^2C_4 \end{bmatrix}.$$
The $\mathcal{C}$ is Hermitian self-dual by Theorem 3.3.
12. Repeat 5. – 11. with different choices of A_{31}, A_{41}, and A_{42}. The Hermitian self-dual linear codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ determined by $\mathcal{C}_0 \subseteq \mathcal{C}_1$ are obtained.

respectively. Then $\mathcal{C}_1$ is Hermitian self-dual and $\mathcal{C}_0 \subseteq \mathcal{C}_1$. Based on Algorithm 1, we have $k = 2$, $l = 1$, $A_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $A_{30} = \begin{bmatrix} \alpha^2 \\ \alpha \end{bmatrix}$, $A_{40} = \begin{bmatrix} \alpha^5 & \alpha^2 \\ 1 & \alpha \end{bmatrix}$, $B_3 = \begin{bmatrix} \alpha^5 \end{bmatrix}$, and $B_{40} = \begin{bmatrix} \alpha & 1 \end{bmatrix}$. Then we have

$$C_4 = -\left(A_{40}^{-1}A_{30}\right)^\dagger = -\left(\begin{bmatrix} \alpha^5 & \alpha^2 \\ 1 & \alpha \end{bmatrix}^{-1} \begin{bmatrix} \alpha^2 \\ \alpha \end{bmatrix}\right)^\dagger = \begin{bmatrix} 0 & 2 \end{bmatrix}.$$

By choosing $A_{31} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, we have $[g_{ij}] = \widetilde{A_{30}A_{31}^\dagger} = \widetilde{\begin{bmatrix} \alpha^2 \\ \alpha \end{bmatrix}\begin{bmatrix} 1 & 1 \end{bmatrix}} = \begin{bmatrix} 0 & \alpha \\ \alpha^3 & 2 \end{bmatrix}$. We choose $x_{11} = 0 \in \{0, \alpha^2, \alpha^6\} = \mathrm{Tr}^{-1}(0) = \mathrm{Tr}^{-1}(-g_{11})$, $x_{22} = 2 \in \{2, \alpha^5, \alpha^7\} = \mathrm{Tr}^{-1}(1) = \mathrm{Tr}^{-1}(-g_{22})$, $x_{21} = 1$, and $x_{12} = -g_{12} - \overline{x_{21}} = -\alpha - 1 = \alpha^3$. It follows that $[x_{ij}] = \begin{bmatrix} 0 & \alpha^3 \\ 1 & 2 \end{bmatrix}$ and $A_{41} = (A_{40}^{-1}[x_{ij}])^\dagger = \begin{bmatrix} 2 & \alpha \\ \alpha & 1 \end{bmatrix}$. Consequently, $B_{41} = -\left(A_{40}^{-1}\left(A_{31}B_3^\dagger + A_{41}B_{40}^\dagger\right)\right)^\dagger = \begin{bmatrix} \alpha & 0 \end{bmatrix}$.

Let $[h_{ij}] = A_{31}A_{31}^{\dagger} + A_{41}A_{41}^{\dagger} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \end{bmatrix} + \begin{bmatrix} \alpha^4 & \alpha \\ \alpha & 1 \end{bmatrix} \begin{bmatrix} \alpha^4 & \alpha^3 \\ \alpha^3 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^3 \\ \alpha & 1 \end{bmatrix}$. *We choose* $y_{11} = 1 \in \{1, \alpha, \alpha^3\} = \mathrm{Tr}^{-1}(2) = \mathrm{Tr}^{-1}(-h_{11})$, $y_{22} = 1 \in \{1, \alpha, \alpha^3\} = \mathrm{Tr}^{-1}(2) = \mathrm{Tr}^{-1}(-h_{22})$, $y_{21} = 1$, *and* $y_{12} = -h_{12} - \overline{y_{21}} = -\alpha^3 - 1 = \alpha$. *Then* $[y_{ij}] = \begin{bmatrix} 1 & a \\ 1 & 1 \end{bmatrix}$ *and* $A_{42} = (A_{40}^{-1}[y_{ij}])^{\dagger} = \begin{bmatrix} \alpha^3 & \alpha^3 \\ 0 & \alpha^5 \end{bmatrix}$.

From Algorithm 1, the matrix

$$\begin{bmatrix} I_k & A_2 & A_{30} + uA_{31} & A_{40} + uA_{41} + u^2A_{42} \\ 0 & uI_l & uB_3 & uB_{40} + u^2B_{41} \\ 0 & 0 & u^2I_l & u^2C_4 \end{bmatrix} = \left[\begin{array}{cc|c|c|cc} 1 & 0 & 1 & \alpha^2+u & \alpha^5+2u+\alpha^3u^2 & \alpha^2+\alpha u+\alpha^3u^2 \\ 0 & 1 & 0 & \alpha+u & 1+\alpha u & \alpha+u+\alpha^5u^2 \\ \hline 0 & 0 & u & \alpha^5u & \alpha u+\alpha u^2 & u \\ \hline 0 & 0 & & u^2 & 0 & 2u^2 \end{array}\right]$$

is a generator matrix for a Hermitian self-dual code of length 6 *over* $\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9$ *with type* $\{2, 1, 1\}$.

When $k = \frac{n}{2}$ in Theorem 3.3 (equivalently, in Algorithm 1), we have the following extension on the parameters of Hermitian self-dual linear codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. Let n be an even positive integer and let $\mathcal{C}_1 = \mathcal{C}_0$ be a Hermitian self-dual code of length n over $\mathbb{F}_q$ with parameters $[n, k = \frac{n}{2}, d]_q$ and generator matrix

$$A = \begin{bmatrix} I_{\frac{n}{2}} & A_{40} \end{bmatrix}, \tag{26}$$

where A_{40} is a $k \times k$ invertible matrix over $\mathbb{F}_q$. Based on Algorithm 1, the linear code $\mathcal{C}$ of length n and type $\{\frac{n}{2}, 0, 0\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix

$$G = \begin{bmatrix} I_k & A_{40} + uA_{41} + u^2A_{42} \end{bmatrix} \tag{27}$$

is Hermitian self-dual. Since $\mathcal{C}$ is a free code, $\mathrm{wt}(\mathcal{C}) = \mathrm{wt}(\mathcal{C}_1) = d$ by [18, Corollary 4.3]. Hence, the following two theorems can be derived directly.

Theorem 3.6. *Let* q *be a prime power and let* n *be an even positive integer. If there exists an* $[n, \frac{n}{2}, \frac{n}{2}+1]_q$ *MDS Hermitian self-dual code over* $\mathbb{F}_q$*, then an MDS Hermitian self-dual code of length* n *over* $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ *of type* $\{\frac{n}{2}, 0, 0\}$ *can be constructed with minimum Hamming weight* $\frac{n}{2} + 1$.

Proof. Assume that there exists an $[n, \frac{n}{2}, \frac{n}{2} + 1]_q$ MDS Hermitian self-dual code $\mathcal{C}_1$ over $\mathbb{F}_q$ with generator matrix of the form (26). By Algorithm 1, a linear code $\mathcal{C}$ of length n and type $\{\frac{n}{2}, 0, 0\}$ over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with generator matrix of the form (27) is Hermitian self-dual. Since $\mathcal{C}$ is free, we have $\mathrm{wt}(\mathcal{C}) = \mathrm{wt}(\mathcal{C}_1) = \frac{n}{2} + 1$ and $\log_{q^3}(|\mathcal{C}|) = \frac{n}{2} = \dim(\mathcal{C}_1)$ by the discussion above. Hence, $\mathrm{wt}(\mathcal{C}) = \frac{n}{2} + 1 = n - \log_{q^3}(|\mathcal{C}|) + 1$ which implies that $\mathcal{C}$ is MDS. $\square$

Using the above theorem, numerous MDS Hermitian self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ can be construct based on known MDS Hermitian self-dual codes over $\mathbb{F}_q$ (see, for example, [13], [17], [24]).

4. Self-dual quasi-abelian codes over principal ideal group algebras

In this section, the study of quasi-abelian codes over principal ideal group algebras is given. In the special case where the field characteristic is 3 and the Sylow 3-subgroup of the underlying finite abelian group has order 3, complete characterization and enumeration of quasi-abelian codes and self-dual quasi-abelian codes are presented in terms linear codes and self-dual linear codes over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ obtained in [3], [4] and Section 3.

4.1. Group rings and quasi-abelian codes

Let R be a finite commutative ring with nonzero identity and let G be a finite abelian group. Then

$$R[G] = \left\{ \sum_{g \in G} \alpha_g Y^g \mid \alpha_g \in R, g \in G \right\}$$

is a commutative ring under the addition and multiplication given for the usual polynomial ring over R with indeterminate Y, where the indices are computed additively in G. The ring $R[G]$ is called a *group ring of* G *over* R. In the case where R is the finite field $\mathbb{F}_{p^m}$, the group ring $\mathbb{F}_{p^m}[G]$ is called a *group algebra of* G *over* $\mathbb{F}_{p^m}$ and it is called a *Principal Ideal Group Algebra (PIGA)* if every ideal in $\mathbb{F}_{p^m}[G]$ is principal. The readers may refer to [15] for more details on group rings. A linear code of length $|G|$ over R can be viewed as an embedded R-submodule of the R-module in $R[G]$ by indexing the $|G|$-tuples by the elements in G. Given a subgroup H of G with index $n = [G : H]$, a linear code $\mathcal{C}$ of length $|G|$ viewed as an R-submodule of $R[G]$ is called an *H-quasi-abelian code* (specifically, an *H-quasi-abelian code of index n*) in $R[G]$ if $\mathcal{C}$ is an $R[H]$-module, i.e., $\mathcal{C}$ is closed under the multiplication by the elements in $R[H]$. Such a code will be called a quasi-abelian code if H is not specified or where it is clear in the context.

Let $\{g_1, g_2, \dots, g_n\}$ be a fixed set of representatives of the cosets of H in G. Let $\mathcal{R} := \mathbb{F}_q[H]$. Define $\Phi : \mathbb{F}_q[G] \to \mathcal{R}^n$ by

$$\Phi\left(\sum_{h \in H} \sum_{i=1}^{n} \alpha_{h+g_i} Y^{h+g_i} \right) = (\alpha_1(Y), \alpha_2(Y), \dots, \alpha_n(Y)),$$

where $\alpha_i(Y) = \sum\limits_{h \in H} \alpha_{h+g_i} Y^h \in \mathcal{R}$ for all $i = 1, 2, \dots, n$. It is well known that Φ is an $\mathcal{R}$-module isomorphism interpreted as follows.

Lemma 4.1 ([10, Lemma 2.1])**.** *The map Φ induces a one-to-one correspondence between H-quasi-abelian codes in $\mathbb{F}_q[G]$ and linear codes of length n over $\mathcal{R}$.*

We note that a group algebra $\mathbb{F}_{p^m}[H]$ is semisimple if and only if the Sylow p-subgroup of H is trivial (see [20, Chapter 2: Theorem 4.2]), and it is a PIGA if and only if he Sylow p-subgroup of H is cyclic (see [6]). In [10], complete characterization and enumeration of H-quasi-abelian codes in $\mathbb{F}_{p^m}[G]$ have been established in the case where $\mathbb{F}_{p^m}[H]$ is semisimple. Here, we focus on a more general case where $\mathbb{F}_{p^m}[H]$ is a PIGA, or equivalently, the Sylow p-subgroup of H is cyclic. Precisely, $H \cong A \times \mathbb{Z}_{p^m i}$ and $G \cong A \times \mathbb{Z}_{p^s} \times B$, where s is a non-negative integer, A and B are finite abelian groups such that $p \nmid |A|$. General characterization is given in Subsection 4.2. In the special case where $p = 3$ and $s = 1$, complete characterization and enumeration of $A \times \mathbb{Z}_3$-quasi-abelian codes and self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ are given in Subsection 4.3.

4.2. $A \times \mathbb{Z}_{p^s}$-Quasi-Abelian Codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$

We focus on H-quasi-abelian codes in $\mathbb{F}_{p^m}[G]$, where $\mathbb{F}_{p^m}[H]$ is a PIGA. Equivalently, $H \cong A \times \mathbb{Z}_{p^s}$ and $G \cong A \times \mathbb{Z}_{p^s} \times B$, where s is a positive integer, A and B are finite abelian groups such that $p \nmid |A|$ (see [6] and [12]).

Note that the group algebra $\mathbb{F}_{p^m}[A]$ is semisimple [2] and it can be decomposed using the Discrete Fourier Transform in [23] (see [12] and [11] for more details). For completeness, the decomposition used in this paper are summarized as follows.

For co-prime positive integers i and j, denote by $\mathrm{ord}_j(i)$ the multiplicative order of i modulo j. For each $a \in A$, denote by $\mathrm{ord}(a)$ the additive order of a in A and the *p^m-cyclotomic class* of A containing

$a \in A$ is defined to be the set

$$S_{p^m}(a) := \{p^{mi} \cdot a \mid i = 0, 1, \dots\} = \{p^{mi} \cdot a \mid 0 \le i < \mathrm{ord}_{\mathrm{ord}(a)}(p^m)\},$$

where $p^{ki} \cdot a := \sum_{j=1}^{p^{mi}} a$ in A. A subset $\{a_1, a_2, \dots, a_t\}$ of A is called a *complete set of representatives* of p^m-cyclotomic classes of A if $S_{p^m}(a_1), S_{p^m}(a_2), \dots, S_{p^m}(a_t)$ are distinct and $\bigcup_{i=1}^{t} S_{p^m}(a_i) = A$.

An *idempotent* in $\mathbb{F}_{p^m}[A]$ is a nonzero element e such that $e^2 = e$. It is called *primitive* if for every other idempotent f, either $ef = e$ or $ef = 0$. The existence of primitive idempotent elements in $\mathbb{F}_{p^m}[A]$ is proved in [5]. They are induced by the p^m-cyclotomic classes of A (see [5, Proposition II.4]). Consequently, $\mathbb{F}_{p^m}[A]$ can be viewed as a direct sum of principal ideals generated by these primitive idempotent elements.

Proposition 4.2 ([5, Corollary III.6])**.** *Let $\{a_1, a_2, \dots, a_t\}$ be a complete set of representatives of p^m-cyclotomic classes of a finite abelian group A where $p \nmid |A|$ and let e_i be the primitive idempotent induced by $S_{p^m}(a_i)$ for all $1 \le i \le t$. Then*

$$\mathbb{F}_{p^m}[A] = \bigoplus_{i=1}^{t} \mathbb{F}_{p^m}[A]e_i \cong \prod_{i=1}^{t} \mathbb{F}_{p^{m_i}},$$

where $m_i = m \cdot \mathrm{ord}_{\mathrm{ord}(a_i)}(p^m)$.

A PIGA $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}]$ can be decomposed in the following theorem.

Theorem 4.3. *Let s be a positive integer. Let $\{a_1, a_2, \dots, a_t\}$ be a complete set of representatives of p^m-cyclotomic classes of a finite abelian group A where $p \nmid |A|$. Then*

$$\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}] \cong \prod_{i=1}^{t} \left(\mathbb{F}_{p^{m_i}} + u\mathbb{F}_{p^{m_i}} + \dots + u^{p^s-1}\mathbb{F}_{p^{m_i}} \right)$$

where $m_i = m \cdot \mathrm{ord}_{\mathrm{ord}(a_i)}(p^m)$ for all $1 \le i \le t$.

Proof. For each $1 \le i \le t$, let e_i be the primitive idempotent induced by $S_{p^m}(a_i)$. From Proposition 4.2, we have

$$\mathbb{F}_{p^m}[A] \cong \mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}]e_i \cong \prod_{i=1}^{t} \mathbb{F}_{p^{m_i}}, \tag{28}$$

and hence,

$$\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}] \cong (\mathbb{F}_{p^m}[A])[\mathbb{Z}_{p^s}] \cong \prod_{i=1}^{t} \mathbb{F}_{p^{m_i}}[\mathbb{Z}_{p^s}]. \tag{29}$$

Under the ring isomorphism that fixes the elements in $\mathbb{F}_{p^{m_i}}$ and $Y^1 \mapsto u+1$, it is not difficult to see that

$$\mathbb{F}_{p^{m_i}}[\mathbb{Z}_{p^s}] \cong \mathbb{F}_{p^{m_i}} + u\mathbb{F}_{p^{m_i}} + \dots + u^{p^s-1}\mathbb{F}_{p^{m_i}} \tag{30}$$

as rings. Therefore,

$$\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}] \cong \prod_{i=1}^{t} \left(\mathbb{F}_{p^{m_i}} + u\mathbb{F}_{p^{m_i}} + \dots + u^{p^s-1}\mathbb{F}_{p^{m_i}} \right) \tag{31}$$

as desired. □

For each finite abelian group B of order n, every $A \times \mathbb{Z}_{p^s}$-quasi-abelian code in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be viewed as a linear code of length n over $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}]$ by Lemma 4.1. The next corollary follows directly from Theorem 4.3.

Corollary 4.4. *Let s and m be positive integers. Let A and B be finite abelian groups such that $|B| = n$ and $p \nmid |A|$. Then every $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be viewed as*

$$\mathcal{C} \cong \prod_{i=1}^{t} \mathcal{C}_i,$$

where $\mathcal{C}_i$ is a linear code of length n over $\mathbb{F}_{p^{m_i}} + u\mathbb{F}_{p^{m_i}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m_i}}$ for all $i = 1, 2, \ldots, t$.

The enumeration of $A \times \mathbb{Z}_{p^s}$-quasi-abelian code in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is given as follows.

Theorem 4.5. *Let s and m be positive integers. Let A and B be finite abelian groups such that $|B| = n$ and the exponent of A is M and $p \nmid M$. Then the number of $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is*

$$\prod_{d|M} \left(N_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}},$$

where $\mathcal{N}_A(d)$ is the number of elements of order d in A determined in [1] and $N_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n)$ is the number of linear codes of length n over $\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}} + u\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}}$ determined in [4, Lemma 2.2].

Proof. From Theorem 4.3, it suffices to determine the number of linear codes of length n over the ring $\mathbb{F}_{p^{m_i}} + u\mathbb{F}_{p^{m_i}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m_i}}$ for all $i = 1, 2, \ldots, t$.

For each divisor d of M, each p^m-cyclotomic class containing an element of order d has $\mathrm{ord}_d(p^m)$ elements and the number of such p^m-cyclotomic classes is $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}$. By Theorem 4.3, it follows that the number of linear codes of length n over $\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}} + u\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m \cdot \mathrm{ord}_d(p^m)}}$ corresponding to d is

$$\left(N_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}}.$$

By taking the summation over all the divisors d of M, the desired result follows. $\square$

Example 4.6. *Let $A \leq H \leq G$ be finite abelian groups such that $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, $H \cong A \times \mathbb{Z}_3$, and $G \cong H \times \mathbb{Z}_4$. Then the 3-cyclotomic classes of A are $S_3((0,0)) = \{(0,0)\}$, $S_3((0,2)) = \{(0,2)\}$, $S_3((1,0)) = \{(1,0)\}$, $S_3((1,2)) = \{(1,2)\}$, $S_3((0,1)) = \{(0,1),(0,3)\}$, and $S_3((1,1)) = \{(1,1),(1,3)\}$. It follows that $\mathrm{ord}_{\mathrm{ord}((0,0))}(3) = \mathrm{ord}_{\mathrm{ord}((0,2))}(3) = \mathrm{ord}_{\mathrm{ord}((1,0))}(3) = \mathrm{ord}_{\mathrm{ord}((1,2))}(3) = 1$ and $\mathrm{ord}_{\mathrm{ord}((0,1))}(3) = \mathrm{ord}_{\mathrm{ord}((1,1))}(3) = 2$. By Proposition 4.2, $\mathbb{F}_3[A]$ has 4 primitive idempotents e_i such that $\mathbb{F}_3[A]e_i \cong \mathbb{F}_3$ and 2 primitive idempotents e_j such that $\mathbb{F}_3[A]e_j \cong \mathbb{F}_9$. Such primitive idempotents are induced by the above 6 cyclotomic classes while their explicit forms can be determined using [5, Proposition II.4]. Consequently,*

$$\mathbb{F}_3[A] \cong \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_9 \times \mathbb{F}_9$$

and

$$\mathbb{F}_3[H] = \mathbb{F}_3[A \times \mathbb{Z}_3] \cong \mathbb{F}_3[\mathbb{Z}_3] \times \mathbb{F}_3[\mathbb{Z}_3] \times \mathbb{F}_3[\mathbb{Z}_3] \times \mathbb{F}_3[\mathbb{Z}_3] \times \mathbb{F}_9[\mathbb{Z}_3] \times \mathbb{F}_9[\mathbb{Z}_3].$$

By Proposition 4.3, we have $\mathbb{F}_3[\mathbb{Z}_3] \cong \mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$ and $\mathbb{F}_9[\mathbb{Z}_3] \cong \mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9$, where $u^3 = 0$. Hence,

$$\mathbb{F}_3[H] \cong \prod_{i=1}^{4}(\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3) \times \prod_{j=1}^{2}(\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9). \tag{32}$$

Using Corollary 4.4, every H-quasi-abelian code in $\mathbb{F}_3[G]$ is isomorphic to a code of the form

$$\mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_4 \times \mathcal{C}_5 \times \mathcal{C}_6,$$

where $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, and $\mathcal{C}_4$ are linear codes of length $|\mathbb{Z}_4| = 4$ over $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, and $\mathcal{C}_5$ and $\mathcal{C}_6$ are linear codes of length 4 over $\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9$.

In the next subsections, we focus on self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ with respect to both the Euclidean and Hermitian inner products.

4.3. Euclidean self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$

Euclidean self-dual $A\times\mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A\times\mathbb{Z}_{p^s}\times B]$ is studied in terms of the following types of p^m-cyclotomic classes. A p^m-cyclotomic class $S_{p^m}(a)$ is said to be of *type* I if $a = -a$ (in this case, $S_{p^m}(a) = S_{p^m}(-a)$), *type* II if $S_{p^m}(a) = S_{p^m}(-a)$ and $a \neq -a$, or *type* III if $S_{p^m}(-a) \neq S_{p^m}(a)$. The primitive idempotent e induced by $S_{p^m}(a)$ is said to be of type $\lambda \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}\}$ if $S_{p^m}(a)$ is a p^m-cyclotomic class of type λ.

Rearrange the terms in the decomposition in Theorem 4.3 based on the p^m-cyclotomic classes of types I, II and III, we have the next theorem.

Theorem 4.7. *Let m and s be positive integers and let A be a finite abelian group such that $p \nmid |A|$. Then*

$$\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}] \cong \left(\prod_{i=1}^{r_{\mathrm{I}}} \mathcal{R}_i\right) \times \left(\prod_{j=1}^{r_{\mathrm{II}}} \mathcal{S}_j\right) \times \left(\prod_{l=1}^{(r_{\mathrm{III}})/2} (\mathcal{T}_l \times \mathcal{T}_l)\right),$$

where $r_{\mathrm{I}}, r_{\mathrm{II}}$ and r_{III} are the numbers of elements in a complete set of representatives of p^m-cyclotomic classes of A of types I, II, and III, respectively, $\mathcal{R}_i = F_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{p^s-1}\mathbb{F}_{p^m}$ for all $i = 1, 2, \ldots, r_{\mathrm{I}}$, $\mathcal{S}_j = \mathbb{F}_{p^{m_{r_{\mathrm{I}}+j}}} + u\mathbb{F}_{p^{m_{r_{\mathrm{I}}+j}}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m_{r_{\mathrm{I}}+j}}}$ for all $j = 1, 2, \ldots, r_{\mathrm{II}}$, and $\mathcal{T}_l = \mathbb{F}_{p^{m_{r_{\mathrm{I}}+r_{\mathrm{II}}+l}}} + u\mathbb{F}_{p^{m_{r_{\mathrm{I}}+r_{\mathrm{II}}+l}}} + \ldots u^{p^s-1}\mathbb{F}_{p^{m_{r_{\mathrm{I}}+r_{\mathrm{II}}+l}}}$ for all $l = 1, 2, \ldots, (r_{\mathrm{III}})/2$.

Using Theorem 4.7 and the analysis similar to those in [11, Section II.D], a $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ and its Euclidean dual are given.

Proposition 4.8. *Let s and m be positive integers. Let A and B be finite abelian groups such that $|B| = n$ and $p \nmid |A|$. Then an $A \times \mathbb{Z}_{p^s}$-quasi-abelian code in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be viewed as*

$$\mathcal{C} \cong \left(\prod_{i=1}^{r_{\mathrm{I}}} \mathcal{B}_i\right) \times \left(\prod_{j=1}^{r_{\mathrm{II}}} \mathcal{C}_j\right) \times \left(\prod_{l=1}^{(r_{\mathrm{III}})/2} (\mathcal{D}_l \times \mathcal{D}'_l)\right), \tag{33}$$

where $\mathcal{B}_i$, $\mathcal{C}_j$, $\mathcal{D}_l$ and $\mathcal{D}'_l$ are linear codes of length n over $\mathcal{R}_i$, $\mathcal{S}_j$, $\mathcal{T}_l$ and $\mathcal{T}_l$, respectively, for all $i = 1, 2, \ldots, r_{\mathrm{I}}$, $j = 1, 2, \ldots, r_{\mathrm{II}}$ and $l = 1, 2, \ldots, (r_{\mathrm{III}})/2$.

Furthermore, the Euclidean dual of $\mathcal{C}$ in (33) is of the form

$$\mathcal{C}^{\perp_{\mathrm{E}}} \cong \left(\prod_{i=1}^{r_{\mathrm{I}}} \mathcal{B}_i^{\perp_{\mathrm{E}}}\right) \times \left(\prod_{j=1}^{r_{\mathrm{II}}} \mathcal{C}_j^{\perp_{\mathrm{H}}}\right) \times \left(\prod_{l=1}^{(r_{\mathrm{III}})/2} \left((\mathcal{D}'_l)^{\perp_{\mathrm{E}}} \times \mathcal{D}_l^{\perp_{\mathrm{E}}}\right)\right).$$

The characterization of Euclidean self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is established in terms of a product of linear codes, Euclidean self-dual linear codes, and Hermitian self-dual linear codes over Galois extensions of the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{p^s-1}\mathbb{F}_{p^m}$.

Corollary 4.9. *Let s and m be positive integers. Let A and B be finite abelian groups such that $|B| = n$ and $p \nmid |A|$. Then a $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is Euclidean self-dual if and only if in the decomposition (33),*

i) $\mathcal{B}_i$ is a Euclidean self-dual linear code of length n over $\mathcal{R}_i$ for all $i = 1, 2, \dots, r_{\mathrm{I}}$,

ii) $\mathcal{C}_j$ is a Hermitian self-dual linear code of length n over $\mathcal{S}_j$ for all $j = 1, 2, \dots, r_{\mathrm{II}}$, and

iii) $\mathcal{D}'_l = \mathcal{D}_l^{\perp_{\mathrm{E}}}$ is a linear code of length n over $\mathcal{T}_l$ for all $l = 1, 2, \dots, (r_{\mathrm{III}})/2$.

From Corollary 4.9, the Euclidean self-duality of $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ depends only on the structure of $A \times \mathbb{Z}_{p^s}$ and the index $n = |B|$ but not the structure of B itself.

Given positive integers m and j, the pair (j, p^m) is said to be *good* if j divides $p^{mt} + 1$ for some positive integer t, and *bad* otherwise. This notion have been introduced in [8] and [11] for the enumeration of self-dual cyclic codes and self-dual abelian codes over finite fields and it is completely determined in [9]. Let χ be a function defined on pairs (j, p^m) as follows.

$$\chi(j, p^m) = \begin{cases} 0 & \text{if } (j, p^m) \text{ is good,} \\ 1 & \text{otherwise.} \end{cases} \tag{34}$$

The number of Euclidean self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be determined as follows.

Theorem 4.10. *Let s and m be positive integers. Let A and B be finite abelian groups such that $|B| = n$ is even and the exponent of A is M and $p \nmid M$. Then the number of Euclidean self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is*

$$(NE_{p^s}(p^m, n))^{\sum\limits_{d|M, \mathrm{ord}_d(p^m)=1} (1-\chi(d,p^m))\mathcal{N}_A(d)} \times \prod_{\substack{d|M \\ \mathrm{ord}_d(p^m) \neq 1}} \left(NH_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{(1-\chi(d,p^m)) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}}$$
$$\times \prod_{d|M} \left(N_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{\chi(d,p^m) \frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^m)}},$$

where $\mathcal{N}_A(d)$ denotes the number of elements in A of order d determined in [1].

Proof. From Corollary 4.9, it suffices to determine the numbers of linear codes $\mathcal{B}_i$'s, $\mathcal{C}_j$'s, and $\mathcal{D}_l$'s such that $\mathcal{B}_i$ and $\mathcal{C}_j$ are Euclidean and Hermitian self-dual, respectively.

From [12, Remark 2.5], the elements in A of the same order are partitioned into p^m-cyclotomic classes of the same type. For each divisor d of M, a p^m-cyclotomic class containing an element of order d has cardinality $\mathrm{ord}_d(p^m)$ and the number of such p^m-cyclotomic classes is $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}$. We consider the following 3 cases.

Case 1: $\chi(d, p^m) = 0$ and $\mathrm{ord}_d(3^k) = 1$. By [11, Remark 2.6], every 3^k-cyclotomic class of A containing an element of order d is of type I. Since there are $\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}$ such p^m-cyclotomic classes, the number of Euclidean self-dual linear codes B_i's of length n corresponding to d is

$$(NE_{p^s}(p^m, n))^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}} = (NE_{p^s}(p^m, n))^{(1-\chi(d,p^m))\mathcal{N}_A(d)}.$$

Case 2: $\chi(d, p^m) = 0$ and $\mathrm{ord}_d(p^m) \neq 1$. By [11, Remark 2.6], every p^m-cyclotomic class of A containing an element of order d is of type II and of even cardinality $\mathrm{ord}_d(p^m)$. Hence, the number of Hermitian self-dual linear codes $\mathcal{C}_j$'s of length n corresponding to d is

$$\left(NH_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}} = \left(NH_{p^s}(p^{m \cdot \mathrm{ord}_d(p^m)}, n) \right)^{(1-\chi(d,p^m)) \frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}}.$$

Case 3: $\chi(d, p^m) = 1$. By [11, Lemma 4.5], every p^m-cyclotomic class of A containing an element of order d is of type $\mathbb{III}$. Then the number of linear codes $\mathcal{D}_l$'s of length n corresponding to d is

$$\left(N_{p^s}(p^{m\cdot \mathrm{ord}_d(p^m)}, n)\right)^{\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^m)}} = \left(N_{p^s}(p^{m\cdot \mathrm{ord}_d(p^m)}, n)\right)^{\chi(d,p^m)\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^m)}}.$$

The formula for the number of Euclidean self-dual $A\times\mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A\times\mathbb{Z}_{p^s}\times B]$ follows since d runs over all divisors of M. $\square$

Remark 4.11. *In general, the numbers $NE_{p^s}(p^m, n)$ and $NH_{p^s}(p^m, n)$ in Theorem 4.10 have not been well studied. In the case where the field characteristic is 3, we have the following conclusions.*

1. *The numbers $N_3(3^m, n)$, $NE_3(3^m, n)$ and $NH_3(3^m, n)$ have been determined in Proposition 2.1, [3, Theorem 1] and Theorem 3.4. By Theorem 4.10, the enumeration for Euclidean self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ is completed. .*
2. *The construction/characterization of linear, Euclidean self-dual and Hermitian self-dual codes of length n over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ have been given in [3], [4] and in the proof of Proposition 3.3. Hence, the construction/characterization of Euclidean self-dual $A \times \mathbb{Z}_3$-quasi-abelian code in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ can be obtained from Corollary 4.9.*
3. *Note that, if n is odd, there are no Hermitian self-dual linear codes of length n over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ by Theorem 3.4. Hence, there are no Euclidean self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ for all abelian groups B of odd order.*

Example 4.12. *Let $A \le H \le G$ be finite abelian groups such that $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, $H \cong A \times \mathbb{Z}_3$, and $G \cong H \times \mathbb{Z}_4$. Form Example 4.6, it is easily seen that the 3-cyclotomic classes $S_3((0,0)) = \{(0,0)\}$, $S_3((0,2)) = \{(0,2)\}$, $S_3((1,0)) = \{(1,0)\}$, $S_3((1,2)) = \{(1,2)\}$ of $A \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ are of type* I, *the 3-cyclotomic classes $S_3((0,1)) = \{(0,1),(0,3)\}$ and $S_3((1,1)) = \{(1,1),(1,3)\}$ are of type $\mathbb{II}$, and there are no 3-cyclotomic classes of type $\mathbb{III}$. Then $r_{\mathrm{I}} = 4$, $r_{\mathbb{II}} = 2$, and $r_{\mathbb{III}} = 0$. In view of Theorem 4.7, (32) is recalled as*

$$\mathbb{F}_3[H] \cong \prod_{i=1}^{4}(\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3) \times \prod_{j=1}^{2}(\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9).$$

Hence, by Corollary 4.9, each Euclidean self-dual H-quasi-abelian code in $\mathbb{F}_3[G]$ is isomorphic to a code of the form

$$\mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_4 \times \mathcal{C}_5 \times \mathcal{C}_6,$$

where $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$, and $\mathcal{C}_4$ are Euclidean self-dual linear codes of length 4 over $\mathbb{F}_3 + u\mathbb{F}_3 + u^2\mathbb{F}_3$, and $\mathcal{C}_5$ and $\mathcal{C}_6$ are Hermitian self-dual linear codes of length 4 over $\mathbb{F}_9 + u\mathbb{F}_9 + u^2\mathbb{F}_9$.

4.4. Hermitian self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$

In this subsection, we focus on the case where m is even and study Hermitian self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$.

The characterization and enumeration of Hermitian self-dual $A\times\mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A\times\mathbb{Z}_{p^s}\times B]$ are given based on the decomposition of a group algebra $\mathbb{F}_{p^m}[A\times\mathbb{Z}_{p^s}]$ in terms of the following types of p^m-cyclotomic classes of A. A p^m-cyclotomic class $S_{p^m}(a)$ is said to be of *type* I' if $S_{p^m}(a) = S_{p^m}(-p^{\frac{m}{2}}a)$ or *type* $\mathbb{II}'$ if $S_{p^m}(a) \neq S_{p^m}(-p^{\frac{m}{2}}a)$. The primitive idempotent e induced by $S_{p^m}(a)$ is said to be of type $\lambda \in \{\mathrm{I}', \mathbb{II}'\}$ if $S_{p^m}(a)$ is a p^m-cyclotomic class of type λ.

Rearrange the terms in the decomposition in Theorem 4.3 based on the p^m-cyclotomic classes of types I' and $\mathbb{II}'$, the next theorem follows.

Theorem 4.13. *Let m be an even positive integer and let A be a finite abelian group such that $p \nmid |A|$.*

$$\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s}] \cong \left(\prod_{j=1}^{r_{\mathrm{I}'}} \mathcal{S} \right) \times \left(\prod_{l=1}^{(r_{\mathrm{II}'})/2} (\mathcal{T}_l \times \mathcal{T}_l) \right),$$

where r_{I}' and $r_{\mathrm{II}'}$ are the numbers of elements in a complete set of representatives of p^m-cyclotomic classes of A of types I' and II', respectively, $\mathcal{S}_j = \mathbb{F}_{p^{m_j}} + u\mathbb{F}_{p^{m_j}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m_j}}$ for all $j = 1, 2, \ldots, r_{\mathrm{I}'}$ and $\mathcal{T}_l = \mathbb{F}_{p^{m_{r_{\mathrm{I}'}+l}}} + u\mathbb{F}_{p^{k_{r_{\mathrm{I}'}+l}}} + \cdots + u^{p^s-1}\mathbb{F}_{p^{m_{r_{\mathrm{I}'}+l}}}$ for all $l = 1, 2, \ldots, (r_{\mathrm{II}'})/2$.

Using Theorem 4.13 and the analysis similar to those in [12, Section II.D], the $A \times \mathbb{Z}_{p^s}$-quasi-abelian code $\mathcal{C}$ in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ and its Hermitian dual are given.

Proposition 4.14. *Let s and m be positive integers such that m is even. Let A and B be finite abelian groups such that $|B| = n$ and $p \nmid |A|$. Then an $A \times \mathbb{Z}_{p^s}$-quasi-abelian code in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be viewed as*

$$\mathcal{C} \cong \left(\prod_{j=1}^{r_{\mathrm{I}'}} \mathcal{C}_j \right) \times \left(\prod_{l=1}^{(r_{\mathrm{II}'})/2} (\mathcal{D}_l \times \mathcal{D}_l') \right), \tag{35}$$

where $\mathcal{C}_j$, $\mathcal{D}_l$ and $\mathcal{D}_l'$ are linear codes of length n over $\mathcal{S}_j$, $\mathcal{T}_l$ and $\mathcal{T}_l$, respectively, for all $j = 1, 2, \ldots, r_{\mathrm{I}'}$ and $l = 1, 2, \ldots, (r_{\mathrm{II}'})/2$.

Furthermore, the Hermitian dual of $\mathcal{C}$ in (35) is of the form

$$\mathcal{C}^{\perp_{\mathrm{H}}} \cong \left(\prod_{j=1}^{r_{\mathrm{I}'}} \mathcal{C}_j^{\perp_{\mathrm{H}}} \right) \times \left(\prod_{l=1}^{(r_{\mathrm{II}'})/2} \left((\mathcal{D}_l')^{\perp_{\mathrm{E}}} \times \mathcal{D}_l^{\perp_{\mathrm{E}}} \right) \right).$$

The characterization of Hermitian self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ in term of a product of linear codes, and Hermitian self-dual linear codes over Galois extensions of the ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{p^s-1}\mathbb{F}_{p^m}$ is established.

Corollary 4.15. *Let s and m be positive integers such that m is even. Let A and B be finite abelian groups such that $|B| = n$ and $p \nmid |A|$. Then an $A \times \mathbb{Z}_{p^s}$-quasi-abelian code in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is Hermitian self-dual if and only if in the decomposition (35),*

i) $\mathcal{C}_j$ is a Hermitian self-dual linear code of length n over $\mathcal{S}_j$ for all $j = 1, 2, \ldots, r_{\mathrm{I}'}$, and

ii) $\mathcal{D}_l' = \mathcal{D}_l^{\perp_{\mathrm{E}}}$ is a linear code of length n over $\mathcal{T}_l$ for all $l = 1, 2, \ldots, (r_{\mathrm{II}'})/2$.

From Corollary 4.15, it follows that the Hermitian self-duality of $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ depends only on the structure of $A \times \mathbb{Z}_{p^s}$ and the index $n = |B|$ but not the structure of B itself.

Given a positive integer m and a positive integer j, the pair (j, p^m) is said to be *oddly good* if j divides $p^{mt} + 1$ for some odd positive integer t. This notion has been introduced in [12] for characterizing the Hermitian self-dual abelian codes in principal ideal group algebra and completely determined in [9].

Let λ be a function defined on the pair (j, p^m) as

$$\lambda(j, p^m) = \begin{cases} 0 & \text{if } (j, p^m) \text{ is oddly good,} \\ 1 & \text{otherwise.} \end{cases} \tag{36}$$

The number of Hermitian self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ can be determined as follows.

Theorem 4.16. *Let s and m be positive integers such that m is even. Let A and B be finite abelian groups such that $|B| = n$ is even and the exponent of A is M and $p \nmid M$. Then the number of Euclidean self-dual $A \times \mathbb{Z}_{p^s}$-quasi-abelian codes in $\mathbb{F}_{p^m}[A \times \mathbb{Z}_{p^s} \times B]$ is*

$$\prod_{d|M} \left(NH_{p^s}(p^{m\cdot \mathrm{ord}_d(p^m)}, p^s) \right)^{(1-\lambda(d,p^{\frac{m}{2}}))\frac{\mathcal{N}_A(d)}{\mathrm{ord}_d(p^m)}} \times \prod_{d|M} \left(N_{p^s}(p^{m\cdot \mathrm{ord}_d(p^m)}, p^s) \right)^{\lambda(d,p^{\frac{m}{2}})\frac{\mathcal{N}_A(d)}{2\mathrm{ord}_d(p^m)}},$$

where $\mathcal{N}_A(d)$ denotes the number of elements of order d in A determined in [1].

Proof. By Corollary 4.15, it is enough to determine the numbers linear codes $\mathcal{C}_j$'s and $\mathcal{D}_l$'s of length n in (35) such that $\mathcal{C}_j$ is Hermitian self-dual. The result can be deduced using arguments similar to those in the proof of Theorem 4.10, where [12, Lemma 3.5] is applied instead of [11, Lemma 4.5]. $\square$

Remark 4.17. *In general, the number $NH_{p^s}(p^m, n)$ of Hermitian self-dual linear codes of length n over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{p^s-1}\mathbb{F}_{p^m}$ in Theorem 4.16 has not been well studied. In the case where the field characteristic is 3, we have the following results.*

1. *The numbers $N_3(p^m, n)$ and $NH_3(3^m, n)$ have been determined in Proposition 2.1 and Theorem 3.4. Hence, the complete enumeration of Hermitian self-dual $A\times\mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A\times\mathbb{Z}_3\times B]$ follows.*

2. *The construction/characterization of linear and Hermitian self-dual dual linear codes of length n over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ have been given in [4] and in the proof of Proposition 3.3. Hence, the construction/characterization of Hermitian self-dual $A \times \mathbb{Z}_3$-quasi-abelian code in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ can be obtained from Corollary 4.15.*

3. *Note that, if n is odd, there are no Hermitian self-dual linear codes of length n over $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ by Theorem 3.4. Hence, there are no Hermitian self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ for all abelian groups B of odd order.*

5. Conclusion and remarks

By extending the technique used in the study of Euclidean self-dual linear codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ in [3], complete characterization and enumeration of Hermitian self-dual linear codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ have been established for all square prime powers q. An algorithm for constructions of such self-dual codes has veen provided as well as an illustrative example. Subsequently, algebraic characterization of H-quasi-abelian codes in $\mathbb{F}_{p^m}[G]$ has been studied, where $H \leq G$ are finite abelian groups and the Sylow p-subgroup of H is cyclic, or equivalently, $\mathbb{F}_{p^m}[H]$ is a principal ideal group algebra. In the special case where $H \cong A \times \mathbb{Z}_3$ with $3 \nmid |A|$, characterization and enumeration of H-quasi-abelian codes and self-dual H-quasi-abelian codes in $\mathbb{F}_{3^m}[H \times B]$ have been completely determined for all finite abelian group B. As applications, characterization and enumeration of self-dual $A \times \mathbb{Z}_3$-quasi-abelian codes in $\mathbb{F}_{3^m}[A \times \mathbb{Z}_3 \times B]$ can be presented in terms of linear codes and self-dual linear codes over some extensions of $\mathbb{F}_{3^m} + u\mathbb{F}_{3^m} + u^2\mathbb{F}_{3^m}$ determined in [3], [4] and Section 3.

In general, it would be interesting to studied $A \times P$-quasi-abelian codes and self-dual $A \times P$-quasi-abelian codes in $\mathbb{F}_{p^m}[A\times P\times B]$ for all primes p and finite abelian p-groups P. For $e \geq 4$, characterization and enumeration of self-dual linear codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{e-1}\mathbb{F}_{p^m}$ are other interesting problems.

Acknowledgment: The authors would like to thank the anonymous referees for their helpful comments.

References

[1] S. Benson, Students ask the darnedest things: A result in elementary group theory, Math. Mag. 70 (1997) 207–211.
[2] S. D. Berman, Semi-simple cyclic and abelian codes, Kibernetika 3 (1967) 21–30.
[3] R. A. Betty, F. Nemenzo, T. L. Vasques, Mass formula for self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, J. Appl. Math. Comput. 57 (2018) 523–546.
[4] Y. Cao, Y. Gao, Repeated root cyclic $\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^l}$, Finite Fields Appl. 31 (2015) 202–227.
[5] C. Ding, D. R. Kohel, S. Ling, Split group codes, IEEE Trans. Inform. Theory 46 (2000) 485–495.
[6] J. L. Fisher, S. K. Sehgal, Principal ideal group rings, Comm. Algebra 4 (1976) 319–325.
[7] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[8] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory 57 (2011) 2243–2251.
[9] S. Jitman, Good integers and some applications in coding theory, Cryptogr. Commun. 10 (2018) 685–704.
S. Jitman, Correction to: Good integers and some applications in coding theory, Cryptogr. Commun. 10 (2018) 1203–1203.
[10] S. Jitman, S. Ling, Quasi-abelian codes, Des. Codes Cryptogr. 74 (2015) 511–531.
[11] S. Jitman, S. Ling, H. Liu, X. Xie, Abelian codes in principal ideal group algebras, IEEE Trans. Info. Theory 59 (2013) 3046–3058.
[12] S. Jitman, S. Ling, P. Solé, Hermitian self-dual abelian codes, IEEE Trans. Info. Theory 60 (2014) 1496–1507.
[13] J.-L. Kim, Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Combinat. Theory A 105 (2004) 79–95.
[14] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, NorthHolland, Amsterdam, 1977.
[15] C. P. Milies, S. K. Sehgal, S. Sehgal, An Introduction to Group Rings, Springer Science Business Media, 2002.
[16] K. Nagata, F. Nemenzo, H. Wada, The number of self-dual codes over $\mathbb{Z}_{p^3}$, Des. Codes Cryptogr. 50 (2009) 291–303.
[17] Y. Niu, Q. Yue, Y. Wu, L. Hu, Hermitian self-dual, MDS, and generalized Reed-Solomon codes, IEEE Commun. Lett. 23 (2019) 781–784.
[18] G. H. Norton, A. Sălăgean, On the Hamming distance of linear codes over a finite chain ring, IEEE Trans. Info. Theory 46 (2000) 1060–1067.
[19] G. H. Norton, A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, AAECC 10 (2000) 489–506.
[20] D. S. Passman, The Algebraic Structure of Group Rings, Wiley, New York, 1977.
[21] V. Pless, On the uniqueness of the Golay codes, J. Comb. Theory 5 (1968) 215–228.
[22] E. M. Rains, N. J. A. Sloane, Self-dual codes. In: Handbook of Coding Theory, pp. 177–294. North-Holland, Amsterdam 1998.
[23] B. S. Rajan, M. U. Siddiqi, Transform domain characterization of abelian codes, IEEE Trans. Inform. Theory 38 (1992) 1817–1821.
[24] H. Tong, X. Wang, New MDS Euclidean and Hermitian self-dual codes over finite fields, Advances in Pure Mathematics 7 (2017) 325–333.